REMARKS/ARGUMENTS

By way of an Office Action dated June 10, 2005, Examiner rejects claims 1-29. Independent claims 1, 12, and 21 were rejected under 35 USC 103(a) as being unpatentable over Price, U.S. Patent No. 6,851,049, in view of Mandelbaum, U.S. Patent No. 5,552,897.

There Is No Motivation To Combine Price and Mandelbaum

Applicant respectfully contends that there is no motivation to combine Price and Mandelbaum. In fact, Price and Mandelbaum teach away from each other. Price is directed to facilitating transmission of email to "an **anonymous recipient** who cannot be identified by examining the email message." (Emphasis added) (Price, Col. 4, lines 55-56). Price further teaches that the anonymous recipient's identity must be protected so that the recipient cannot be uniquely identified. Price (Col 4, lines 57-60). In contrast, Mandelbaum is directed to the secure transmission of messages to identifiable known users. In Mandelbaum, the message header "**which identifies an intended recipient**" (Mandelbaum, Col 2, line 13), is "**unrestricted**" Mandelbaum, Col 1, lines 65-66), and available to "**all who care to know**." (Emphasis added) (Mandelbaum, Col 2, lines 18-19). Further, Mandelbaum teaches that fax documents are provided with restricted and unrestricted portions. The unrestricted portion identifies the message recipient. (Mandelbaum, Col 1, line 63 through Col 2, line 2).

Further, Mandelbaum is limited to encrypting message using "recipient's public key K_{RP} or sender's private key K_{SS}". (Mandelbaum, Col 2, lines 32-36). However, Price is limited to encrypting the message with the recipient's public key and decrypting

message with the recipient's private key. Very clearly, Price requires that "Recipients hold private keys. . . . These private keys enable recipients to decrypt email messages that have been encrypted with corresponding public keys." (Price, Col 3, line 65 through Col 4, line 2).

Further, Price is designed to keep the recipient identity anonymous. (Price, Col. 4, lines 55-56). Specifically, Price is directed to an "anonymous recipient who cannot be identified by examination the email message." (Price, Col. Lines 55-56). Mandelbaum, however, requires that the recipient's identification is available to "all who care to know." (Mandelbaum, Col 2, lines 18-19). In Mandelbaum, the message header "**which identifies an intended recipient**" (Mandelbaum, Col 2, line 13), is "**unrestricted**" Mandelbaum, Col 1, lines 65-66), and available to "**all who care to know**." (Emphasis added) (Mandelbaum, Col 2, lines 18-19). Further, Mandelbaum requires that the identify of the recipient be known as the "Recipient List", "Typical Header Message", and "Header Messages" lists all require the recipient identification and even fax number to be contained in the list. (Mandelbaum, Figure 4).

Therefore, since Price is intended to "protect the identity of anonymous recipient" (Price, Col 4, line 57) and Mandelbaum shares the identify of the recipient with "all who care to know." (Mandelbaum, Col 2, lines 18-19), the combination of Price and Mandelbaum would destroy the purpose of Price. Further, such a combination would make Mandelbaum inoperable since Mandelbaum cannot be restricted to simply encrypting the message with the recipient's public key and requiring that the decryption occur with the recipient's private key. Therefore, Price and Mandelbaum cannot be combined and specifically teach away from combination.

As such, Applicant respectfully contends that the 103(a) rejection is improper. Applicant respectfully requests that Examiner withdraw the 103(a) rejection and grant a notice of allowance for claims 1-29 in the normal course of Patent Office business.

Price, alone or in combination with Mandelbaum,
does not anticipate the independent claims of the present invention

Even if it were possible to combine Price and Mandelbaum, the references, alone or in combination, do not anticipate or render obvious the claims of the present invention. As an initial matter, Applicant would like to point out that Price is not directed to solve the same problem as that of the present invention. Price is designed to provide "system that facilitates secure transmission of an email message to **anonymous recipients** without divulging the identities of the **anonymous recipients**." (Emphasis added) (Price, Abstract). Price is not directed to an invention that allows for secure message transmissions to recipients that are not part of the secured transmission system.

Specifically, Price requires that "a corresponding private key **held by the recipient** can be used to decrypt the encrypted session key." (Price, Abstract). Price specifically requires that the private key be held by the recipient to decrypt the message "only a corresponding private key **held by the recipient** can be used to decrypt the encrypted session key". (Emphasis added) (Price, Col2, lines 28-30). Price is very clear in that the invention requires that:

> Recipients hold private keys, respectively. These private keys enable recipients to decrypt email messages that have been encrypted with corresponding public keys.
> (Price, Col 3, line 65 through Col 4, line 2).

Further, in each of the embodiments described in Price, the recipient must have a public and private key to decrypt the message and therefore, must be a member of an encryption system. For example, in the first embodiment, Price states that each recipient has the session key encrypted with "a public key associated with the recipient" (Price, Col 2, lines 27); in the second embodiment, "public keys belonging to anonymous recipients" (Price, Col 2, lines 40); in the third embodiment, "a public key belonging to an anonymous recipient is additionally modified" (Price, Col 2, lines 48-49); in the fourth embodiment, "that a recipient can examine the checksum to verify that the correct private key was used" (Price, Col 2, line58-59); and in the last embodiment Price discloses that each "of these entries contains the session key encrypted with a public key associated with the recipient." (Price, Col. 3, lines 1-2). Therefore, Price expressly requires that the recipient has a public and private key and therefore requires that the recipient be a member of an encryption system since Price requires access to the recipient's public and private key.

In the present invention, the non-member recipient does not need to have a public and private key, as encryption keys are generated for the message upon discovering that the recipient is a non-member of the encryption system. Therefore Prices does not anticipate the independent claims of the present invention pursuant to 35 U.S.C. § 102 or 35 U.S.C. § 103.

Further, the recipient does not hold key pairs as these are generated and encrypted in the present invention and are not transmitted to the recipient. In fact, one advantage of the present invention is that the non-member recipient does not have to have a public or private key, does not have to maintain such a key pair, and need not be

a member of an encryption system. Specifically, the present invention is directed to secured messaging for recipients that are not part of an encryption system and do not have to have a public/private key pair through an encryption system. In the present invention, the recipient does not have encryption pairs transmitted to the recipient so that the keys are not known to the recipient as required by Price.

For clarification, the Applicant notes that the "session key" of Price (Price, Col 1, line 50-53) is not the generated encryption keys of the present invention. As disclosed in Price, "a session key (that is randomly selected for the message) . . . is then encrypted with the public key of each of the recipients." (Price, Col 1, lines 51-56). In the present invention, there is not a randomly selected session key but rather generated encryption keys when a recipient is discovered to be a non-member of the encryption system.

Further, Price requires that "key identifiers for the public keys [for the recipient] are sent along with the encrypted session keys, so that each recipient can determine whether or not the recipient possesses a corresponding private key that can decrypt the encrypted session key." (Price, Col 1, lines 59-63). In the present invention, the recipient does not need to have a public or private key as the recipient in the present invention is discovered to be a non-member of an encryption system.

As stated above, Price does not teach the encryption of a generated key pair in response to discovering that a recipient is a non-member to an encryption system. Further, Price requires that the recipient have a public and private key and therefore requires that the recipient be a member of an encryption system. The system described in the present invention eliminates the need for a recipient to be a member of an

encryption system and have a public and private key. Rather, the present invention does not rely upon the need for the recipient to have been assigned a public key of private key from a Certificate Authority in order to receive encrypted messages.

Respectfully, since Price does not claim or disclose the present invention and therefore does not anticipate the independent claims, and associated dependent claims, under 35 U.S.C. § 102.

Mandelbaum, alone or in combination with Price,
does not anticipate the independent claims of the present invention

Mandelbaum is not directed to and does not claim or disclosure the use of generated encryption keys for messages sent to non-member recipients. Like Price, Mandelbuam requires that the recipient be a member of an encryption system and have encryption keys. The encryption method of Mandelbaum is limited to only two encryption methods: "encrypted messages may be encrypted on **one of two different ways** – for example, by using the recipient's public key K_{RP} (K_{RP} encrypt flag is 1) or by using a sender's private key K_{SS} (K_{SS} encrypt flag is 1). (Mandelbaum, Col 4, lines 44-47). Further, these keys are stored and must be obtained from the smart card data in possession by the sender. (Mandelbaum, Col 4, lines 48-49). Specifically, Mandelbaum is limited to retrieving the sender's or recipient's keys from "Table 401" (recipient list) or "Table 402" (smart card owner's data). (Mandelbaum, Col 4, lines 48-49 and Figure 4). Therefore, Mandelbaum requires that the sender and recipient be members of the encryption system since the only two encryption systems require that the sender or recipient have encryption keys.

In the present invention, the keys used to encrypt the message are generated for the message and for the recipient and are not retrieved from any table. Specifically, the non-member recipient is not part of the encryption system and does not have a public or private key pair in which to use to encrypt the message sent to the non-member recipient.

Further, Mandelbaum is limited to a header message associated with the message to be transmitted which contains the "recipient's public key encrypt flag (K_{RP}) and sender's private key encrypt flag (K_{SS}). (Mandelbaum, Col 4, lines 56-57). Therefore, Mandelbaum requires that the sender and recipient be members of an encryption system since the both sender and recipient have encryption keys. In the present invention, the recipient is a non-member to the encryption system and therefore keys used to encrypt the message are generated when it is discovered that the recipient is a non-member. The present invention does not use existing public and private keys associated with the recipient.

Notably, neither Price or Mandelbaum, alone or in combination, are able to send encrypted message to non-members since both reference require that the sender and recipient have encryption keys therefore requiring both sender and recipient to belong to an encryption system. As such, neither Price or Mendlebaum, alone or in combination anticipate the presenting invention or make obvious the present invention under 35 U.S.C. §§ 102 or 103.

Mandelbaum Nor Price, Alone Or In Combination Disclose A Pass-Phrase As Claimed In The Present Invention

The Office action states that Mandelbaum discloses the use of a password to decrypt the message. Respectfully, the present invention does not decrypt the message using the pass-phrase but only decrypts the generated encryption keys. As claimed in the present invention, the pass-phrase is used to decrypt the generated key pair that was generated and used to decrypt the transmitted message and does not decrypt the message itself.

Mandelbaum, on the other hand, only claims or discloses the use of a password to be used in combination with a login to gain access to a message, not to decrypt the message (Mandelbaum, Col 2, lines 2-7). Encryption of message by Mandelbaum are preformed through the "recipient's public key K_{RP} or sender's private key K_{SS}". (Mandelbaum, Col 2, lines 32-36). Further, Mandelbaum does not claim or disclose the decryption of keys which are then used to decrypt a message from such generated keys, generated when a recipient is discovered to be a non-member of the encryption system.

Mandelbaum also places the recipient and sender's keys in the message header. (Mandlebaum, Figure 4). As such, Mendelbaum requires that the recipient and sender be member of an encryption system since this information in contained in the message header.

Therefore, the claims, as amended, are not anticipated by Price or Mandelbaum, alone or in combination, since neither reference claims or discloses the generation of key pairs for encrypting a message for transmission to a no-member recipient of the

encryption system, encrypting the key pair according to an encryption pass-phrase, decrypting the encrypted key pair upon receiving the encryption pass-phrase.

Conclusion

Applicant respectfully believes that the independent claims and the associated dependent claims are now in a condition for allowance and respectfully requests that Examiner issue a notice of allowance for this claim and those depending from it in the normal course of business of the PTO. Applicant respectfully requests that these claims be issued in the normal course of PTO business.

Applicant respectfully submits new claims 30-33 for consideration. Applicant believes these claims to be in condition for allowance as well for the reasons stated above, among others.

Respectfully submitted,

Douglas W. Kim
Registration No. 44,828
McNair Law Firm, P.A.
P.O. Box 10827
Greenville, SC 29603-0827
Telephone: (864) 232-4261
Attorney for the Applicant